VALKYRIE COMODO

Summary

File Name: 176928788.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

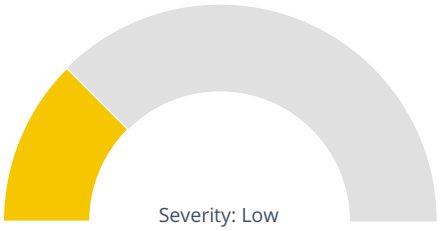
SHA1: aa45509ac9b2d11e55784eddc52f966444d77099

MD5: a47573d164d84977ae6adf3db7119c4e

PUA

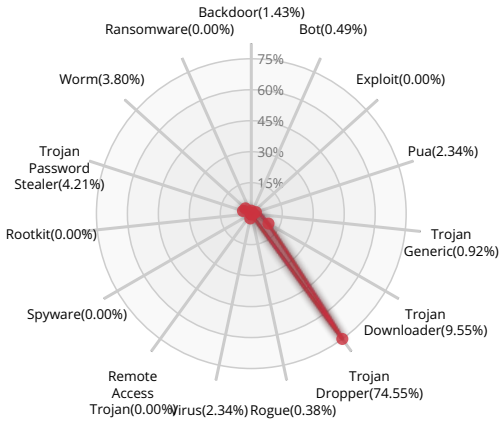
Valkyrie Final Verdict

DETECTION SECTION

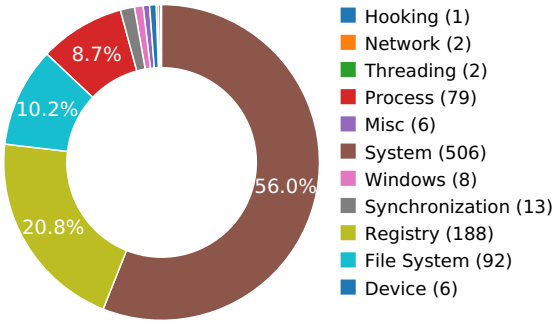


Verdict: PUA

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

NETWORKING

Performs some HTTP requests — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Attempts to restart the guest VM — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

VALKYRIE COMODO

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\netmsg.dll
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\aa45509ac9b2d11e55784eddc52f966444d77099.exe
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\is-7GR0E.tmp
C:\Users\user\AppData\Local\Temp\is-7GR0E.tmp\aa45509ac9b2d11e55784eddc52f966444d77099.tmp
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\is-7GR0E.tmp\netmsg.dll
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp_isetup
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp\license.key
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp\license.ENU
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp\license.ENU.DLL
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp\license.EN
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp\license.EN.DLL
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp*
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp_isetup*

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\A2D5EDFB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegSvcs0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegProcs0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\JSCount
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\ESCount
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RRCount
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Reliability\ShutdownIgnorePredefinedReasons

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\is-7GR0E.tmp\aa45509ac9b2d11e55784eddc52f966444d77099.tmp
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp\license.key

RESOLVED APIS

kernel32.dll.SetDllDirectoryW
kernel32.dll.SetSearchPathMode
kernel32.dll.SetProcessDEPPolicy
kernel32.dll.Wow64DisableWow64FsRedirection
kernel32.dll.Wow64RevertWow64FsRedirection
kernel32.dll.GetUserDefaultUILanguage
comctl32.dll.RegisterClassNameW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
dwmapi.dll.DwmIsCompositionEnabled
uxtheme.dll.EnableThemeDialogTexture
advapi32.dll.UnregisterTraceGuids
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
gdi32.dll.GdiIsMetaPrintDC

ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
cryptbase.dll.SystemFunction036
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
uxtheme.dll.OpenThemeData
uxtheme.dll.CloseThemeData
uxtheme.dll.DrawThemeBackground
uxtheme.dll.DrawThemeText
uxtheme.dll.GetThemeBackgroundContentRect
uxtheme.dll.GetThemePartSize
uxtheme.dll.GetThemeTextExtent
uxtheme.dll.GetThemeTextMetrics
uxtheme.dll.GetThemeBackgroundRegion
uxtheme.dll.HitTestThemeBackground
uxtheme.dll.DrawThemeEdge
uxtheme.dll.DrawThemeIcon
uxtheme.dll.IsThemePartDefined
uxtheme.dll.IsThemeBackgroundPartiallyTransparent
uxtheme.dll.GetThemeColor
uxtheme.dll.GetThemeMetric
uxtheme.dll.GetThemeString
uxtheme.dll.GetThemeBool
uxtheme.dll.GetThemeInt
uxtheme.dll.GetThemeEnumValue
uxtheme.dll.GetThemePosition
uxtheme.dll.GetThemeFont
uxtheme.dll.GetThemeRect
uxtheme.dll.GetThemeMargins
uxtheme.dll.GetThemeIntList
uxtheme.dll.GetThemePropertyOrigin
uxtheme.dll.SetWindowTheme
uxtheme.dll.GetThemeFilename
uxtheme.dll.GetThemeSysColor

uxtheme.dll.GetThemeSysColorBrush
uxtheme.dll.GetThemeSysBool
uxtheme.dll.GetThemeSysSize
uxtheme.dll.GetThemeSysFont
uxtheme.dll.GetThemeSysString
uxtheme.dll.GetThemeSysInt
uxtheme.dll.IsThemeActive
uxtheme.dll.IsAppThemed
uxtheme.dll.GetWindowTheme
uxtheme.dll.IsThemeDialogTextureEnabled
uxtheme.dll.GetThemeAppProperties
uxtheme.dll.SetThemeAppProperties
uxtheme.dll.GetCurrentThemeName
uxtheme.dll.GetThemeDocumentationProperty
uxtheme.dll.DrawThemeParentBackground

DELETED FILES

C:\Users\user\AppData\Local\Temp\is-7GR0E.tmp\aa45509ac9b2d11e55784eddc52f966444d77099.tmp
C:\Users\user\AppData\Local\Temp\is-7GR0E.tmp
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp\license.key
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp_isetup
C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\aa45509ac9b2d11e55784eddc52f966444d77099.tmp
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledProcesses\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\A2D5EDFB
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledSessions\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_CURRENT_USER\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegSvcs0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegProcs0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\JSCount
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\ESCount
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RRCount
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Reliability
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Reliability\ShutdownIgnorePredefinedReasons
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Reliability\UserDefined\1033

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\is-7GR0E.tmp\aa45509ac9b2d11e55784eddc52f966444d77099.tmp" /SL5="$E01A2,140401,58744,C:\Users\user\AppData\Local\Temp\aa45509ac9b2d11e55784eddc52f966444d77099.exe"

"shutdown.exe" -r -f -t 0

READ FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui

C:\Windows\System32\netmsg.dll

C:\Users\user\AppData\Local\Temp\aa45509ac9b2d11e55784eddc52f966444d77099.exe

C:\Windows\Globalization\Sorting\sortdefault.nls

C:\Windows\Fonts\staticcache.dat

\Device\KsecDD

C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp_isetup_setup64.tmp

C:\Users\user\AppData\Local\Temp\is-2I3F7.tmp\license.key

MUTEXES

CicLoadWinStaWinSta0

Local\MSCTF.CtfMonitorInstMutexDefault1

Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511

Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000

Inno

MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000

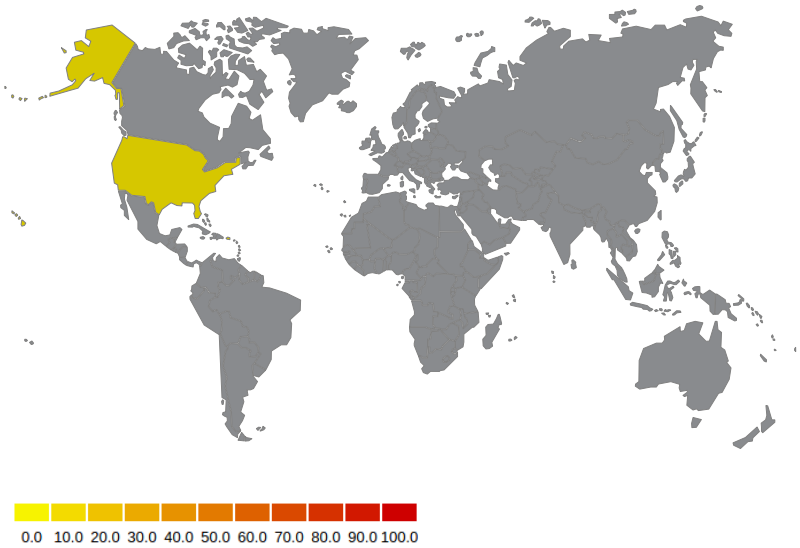
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner

HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash

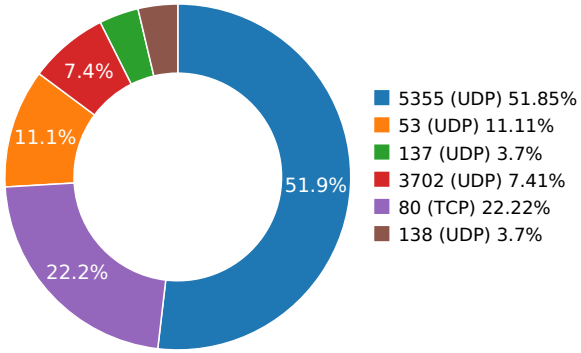
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Communications, Inc.	Malware Process
	23.67.250.139	United States	20940	Akamai Technologies, Inc.	Malware Process
	23.67.250.18	United States	20940	Akamai Technologies, Inc.	OS Process
	23.218.156.64		20940	Akamai Technologies, Inc.	OS Process
	23.67.250.154		20940	Akamai Technologies, Inc.	Malware Process
	23.67.250.17		20940	Akamai Technologies, Inc.	OS Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.msftncsi.com	80	GET	1.1	Microsoft NCSI	1	40.2993140221
Path: /ncsi.txt **URI:** http://www.msftncsi.com/ncsi.txt						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	369.751300812
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?3ed7f7e5fbdcae60 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?3ed7f7e5fbdcae60						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	375.149554968
Path: /pki/crl/products/CSPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/CSPCA.crl						

DNS QUERIES

Request	Type
www.msftncsi.com	A
Answers - www.msftncsi.com.edgesuite.net (CNAME) - 23.67.250.139 (A) - 23.67.250.121 (A) - a1961.g2.akamai.net (CNAME)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 23.67.250.24 (A) - 23.67.250.17 (A) - a1621.g.akamai.net (CNAME) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
crl.microsoft.com	A
Answers - a1363.dscg.akamai.net (CNAME) - crl.www.ms.akadns.net (CNAME) - 23.67.250.18 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
40.2993140221	Sandbox	23.67.250.139	80
369.751300812	Sandbox	23.67.250.17	80
375.149554968	Sandbox	23.67.250.18	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.19671082497	Sandbox	224.0.0.252	5355
3.21772003174	Sandbox	224.0.0.252	5355
3.22354793549	Sandbox	239.255.255.250	3702
3.26599502563	Sandbox	192.168.56.255	137
5.78115487099	Sandbox	224.0.0.252	5355
9.26417303085	Sandbox	192.168.56.255	138
31.4714858532	Sandbox	224.0.0.252	5355
34.6368119717	Sandbox	239.255.255.250	3702
35.6395959854	Sandbox	224.0.0.252	5355
37.6865999699	Sandbox	224.0.0.252	5355
38.2199659348	Sandbox	224.0.0.252	5355
40.2512550354	Sandbox	8.8.4.4	53
40.7790989876	Sandbox	224.0.0.252	5355
43.3421239853	Sandbox	224.0.0.252	5355
45.9042739868	Sandbox	224.0.0.252	5355
364.301962852	Sandbox	224.0.0.252	5355
366.885892868	Sandbox	224.0.0.252	5355
369.498893976	Sandbox	8.8.4.4	53
369.933310032	Sandbox	224.0.0.252	5355
372.491599798	Sandbox	224.0.0.252	5355
375.0454638	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-7GR0E.Tmp\Aa45509ac9b2d11e55784eddc52f966444d77099.Tmp	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 832dab307e54aa08f4b6cdd9b9720361 **SHA-1 :** ebd007fb7482040ecf34339e4bf917209c1018df **SHA-256 :** cc783a04ccbca4edd06564f8ec88fe5a15f1e3bb2 **SHA-512 :** 358d43522fd460eb1511708e4df22ea454a95e5b **Size :** 713.728 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-2I3F7.Tmp_isetup_setup64.Tmp	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** e4211d6d009757c078a9fac7ff4f03d4 **SHA-1 :** 019cd56ba687d39d12d4b13991c9a42ea6ba03da **SHA-256 :** 388a796580234efc95f3b1c70ad4cb44bfddc7ba **SHA-512 :** 17257f15d843e88bb78adcfb48184b8ce22109cc **Size :** 6.144 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-2I3F7.Tmp\License.Key	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** d82a429efd885ca0f324dd92afb6b7b8 **SHA-1 :** 86bbdaa15e6fc5c7779ac69c84e53c43c9eb20ea **SHA-256 :** b258c4d7d2113dee2168ed7e35568c8e03341e2 **SHA-512 :** 5bf0c3b8fa5db63205a263c4fa5337188173248b **Size :** 205.312 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	176928788.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	aa45509ac9b2d11e55784eddc52f966444d77099
MD5:	a47573d164d84977ae6adf3db7119c4e
First Seen Date:	2017-12-23 18:52:36.410654 (about a year ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-12-23 18:52:36.410654 (about a year ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	8
Trid	[[77.7, u'Inno Setup installer'], [10.0, u'Win32 Executable Delphi generic'], [4.6, u'Win32 Dynamic Link Library (generic)'], [3.1, u'Win32 Executable (generic)'], [1.4, u'Win16/32 Executable Delphi generic']]
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
LegalCopyright	
FileVersion	
CompanyName	
Comments	This installation was built with Inno Setup.
ProductName	____
ProductVersion	1.2
FileDescription	
Translation	0x0000 0x04b0
Entry Point	0x40aa98 (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	388198
Ssdeep	6144:XP7OoIlvnL8+Ee0CYDxbGKls0flazlqSXbAkuWxJEknSGZMxhSLupnmd/tnl05i:/7bIlvnL8+iDR/67azlqqnHTEknjMxIT
Sha256	1f5267c16780258388ef8ad44ee302fb0fe4fc557de93150787deb67bb101f8c
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/a/a/4/5/aa45509ac9b2d11e55784eddc52f966444d77099', u'EXE:ProductName': u'____ ', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2017:12:23 18:52:23+00:00', u'EXE:InitializedDataSize': 17920, u'File:FileModifyDate': u'2017:12:23 18:52:22+00:00', u'EXE:FileVersionNumber': u'0.0.0.0', u'EXE:FileVersion': u' ', u'File:FileSize': u'379 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'1.2 ', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u' ', u'File:FileName': u'aa45509ac9b2d11e55784eddc52f966444d77099', u'EXE:ImageVersion': 6.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 1.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'1992:06:19 22:22:17+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u' ', u'EXE:LinkerVersion': 2.25, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/a/a/4/5', u'EXE:FileDescription': u'', u'EXE:EntryPoint': u'0xaa98', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 41472, u'EXE:Comments': u'This installation was built with Inno Setup.', u'File:FileInodeChangeDate': u'2017:12:23 18:52:23+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'0.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	b9a08f46a1a607d0dccfe0d020e621c1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0xa1d0	0xa200	6.63550844572	a49ce5969afc99027d2ca29c05b382dc
DATA	0xc000	0x250	0x400	2.74012451302	9b2268ed5360951559d8041925d025fb
BSS	0xd000	0xe94	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xe000	0x97c	0xa00	4.47624034315	680e72267857783c13b81c8d773f04e9
.tls	0xf000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x10000	0x18	0x200	0.245146276048	3562a9a4f904acbe99cae8308cf0e38a
.reloc	0x11000	0x91c	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x12000	0x2f9d	0x2c00	4.5678230775	f470b4f8bb4fb2768259d85c98e94683

PE Imports

- kernel32.dll
  - DeleteCriticalSection
  - LeaveCriticalSection
  - EnterCriticalSection
  - InitializeCriticalSection
  - VirtualFree
  - VirtualAlloc
  - LocalFree
  - LocalAlloc
  - WideCharToMultiByte
  - TlsSetValue
  - TlsGetValue
  - MultiByteToWideChar
  - GetModuleHandleA
  - GetLastError
  - GetCommandLineA
  - WriteFile
  - SetFilePointer
  - SetEndOfFile
  - RtlUnwind
  - ReadFile
  - TlsAlloc
  - GetStdHandle
  - GetFileSize
  - GetSystemTime
  - GetFileType
  - ExitProcess
  - CreateFileA
  - CloseHandle
- user32.dll
  - MessageBoxA
- oleaut32.dll
  - VariantChangeTypeEx
  - VariantCopyInd
  - VariantClear
  - SysStringLen
  - SysAllocStringLen
- advapi32.dll
  - RegQueryValueExA
  - RegOpenKeyExA
  - RegCloseKey
  - OpenProcessToken
  - LookupPrivilegeValueA
- kernel32.dll
  - WriteFile
  - VirtualQuery
  - VirtualProtect
  - VirtualFree
  - VirtualAlloc
  - Sleep
  - SizeofResource
  - SetLastError

    - SetFilePointer
    - SetErrorMode
    - SetEndOfFile
    - RemoveDirectoryA
    - ReadFile
    - LockResource
    - LoadResource
    - LoadLibraryA
    - IsDBCSLeadByte
    - GetWindowsDirectoryA
    - GetVersionExA
    - GetVersion
    - GetUserDefaultLangID
    - GetSystemInfo
    - GetSystemDirectoryA
    - GetSystemDefaultLCID
    - GetProcAddress
    - GetModuleHandleA
    - GetModuleFileNameA
    - GetLocaleInfoA
    - GetLastError
    - GetFullPathNameA
    - GetFileSize
    - GetFileAttributesA
    - GetExitCodeProcess
    - GetEnvironmentVariableA
    - GetCurrentProcess
    - GetCommandLineA
    - GetACP
    - InterlockedExchange
    - FormatMessageA
    - FindResourceA
    - DeleteFileA
    - CreateProcessA
    - CreateFileA
    - CreateDirectoryA
    - CloseHandle
- user32.dll
    - TranslateMessage
    - SetWindowLongA
    - PeekMessageA
    - MsgWaitForMultipleObjects
    - MessageBoxA
    - LoadStringA
    - ExitWindowsEx
    - DispatchMessageA
    - DestroyWindow
    - CreateWindowExA
    - CallWindowProcA
    - CharPrevA
- comctl32.dll
    - InitCommonControls
- advapi32.dll
    - AdjustTokenPrivileges

PE Resources

{u'lang': u'LANG_DUTCH', u'name': u'RT_ICON', u'offset': 74580, u'sha256': u'f59f62e7843b3ff992cf769a3c608acd4a85a38b3b302cda8507b75163659d7b', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_DUTCH', u'name': u'RT_ICON', u'offset': 74876, u'sha256': u'dc785b2a3e4ea82bd34121cc04e80758e221f11ee686fcfd87ce49f8e6730b22', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_DUTCH', u'name': u'RT_ICON', u'offset': 76260, u'sha256': u'ca8fc96218d0a7e691dd7b95da05a27246439822d09b829af240523b28fd5bb3', u'type': u'data', u'size': 744}

{u'lang': u'LANG_DUTCH', u'name': u'RT_ICON', u'offset': 77004, u'sha256': u'3bbacbad1458254c59ad7d0fd9bea998d46b70b8f8dcfc56aad561a293ffdae3', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 79220, u'sha256': u'2c0d32398e3c95657a577c044cc32fe24fa058d0c32e13099b26fd678de8354f', u'type': u'data', u'size': 754}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 79976, u'sha256': u'840989e0a92f2746ae60b8e3efc1a39bcca17e82df3634c1643d76141fc75bb3', u'type': u'data', u'size': 780}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 80756, u'sha256': u'26bda4da3649a575157a6466468a0a8694475664385595412 0fd715f3c9c7f78', u'type': u'data', u'size': 718}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 81476, u'sha256': u'd786490af7fe66042fb4a7d52023f5a1442f9b5e65d067b9093d1a128a6af34c', u'type': u'data', u'size': 104}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 81580, u'sha256':

u'00a0794f0a493c167f64ed8b119d49bdc59f76bb35e5c295dc047095958ee2fd', u'type': u'data', u'size': 180}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 81760, u'sha256': u'34973a8a33b90ec734bd328198311f579666d5aeb04c94f469ebb822689de3c3', u'type': u'data', u'size': 174}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 81936, u'sha256': u'13d4b048fb409d392cf3457c5135899477ed8c44fdd17abbe6dbe3f3bf88dfd8', u'type': u'data', u'size': 44}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 81980, u'sha256': u'44b095a62d7e401671f57271e6cada367bb55cf7b300ef768b3487b841facd3c', u'type': u'MS Windows icon resource - 4 icons, 16x16, 16 colors', u'size': 62}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 82044, u'sha256': u'd1d9016a2739c0625c90e2b78a2ae68f8203f22f0078f6d5d9f12e6c126f323f', u'type': u'data', u'size': 1268}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 83312, u'sha256': u'356ca8abf11d97bf9dcbff47c04bf1ddcb8685ef84d38e6850ec6c28a37655b9', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 1580}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS